

# Current Threats & Countermeasures



## Speakers:

- **David Bonvillain** – Accuvant Director of Assessment Services
- **Jim Broome** – Accuvant Assessment Technical Lead and Principal Assessor



"Oh hey! I just love these things! ... Crunchy on the outside and a chewy center!"



# Agenda

---

- The Changing Landscape of Security Architectures
- Modern Attack Vectors
  - Google
    - Data Mining and Target Identification
  - Attack Frameworks
  - Wireless Networks
    - Bypassing Security Controls
  - Web Applications
    - Application attacks from Information Gathering to Exploitation
  - Physical Security
    - Lockpicking for the lazy/efficient
  - VoIP
    - Spoofing, Monitoring and Phishing
  - RFID Hacking
- Solutions and Mitigation Strategies

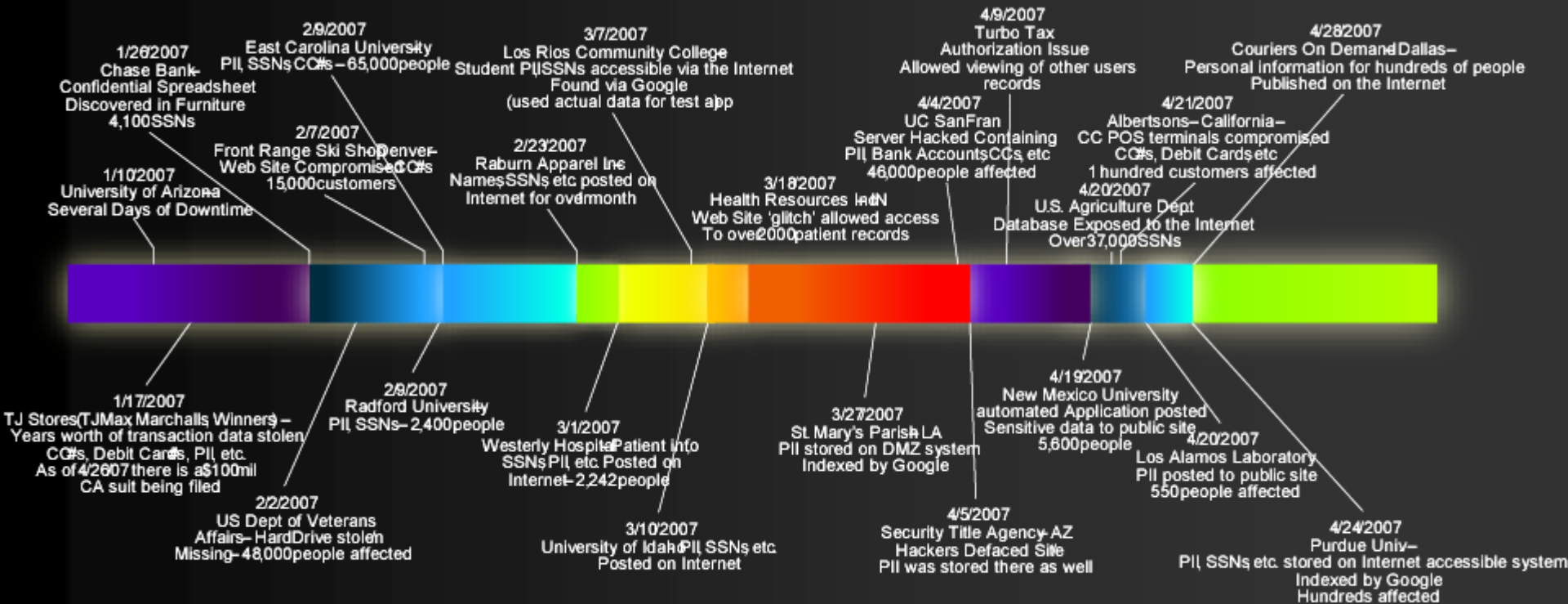
# Since January 1, 2007...

---

Over 121+ known instances of  
privacy violation via:

- Data Security Breach / Intrusions
- Theft
- Inappropriate Use of Data

# The Information Security Problem



# In the News

## Records of 2,000 Westerly Hospital patients posted online

AP Associated Press

March 1, 2007

WESTERLY, R.I. --Two-thousand patients at Westerly Hospital had their names, Social Security numbers and medical records posted on a publicly accessible Web site, and the hospital said it doesn't know who did it.

"We don't know why it happened. We don't know how it happened," said President and CEO of Westerly Sun.

The Web site includes information about patients' surgical medical histories, as well as addresses and insurance

The hospital said not affected, and the breach to patients seen during January. The Sun reported contacted had been

Westerly Police learned a woman looked up the Google and found a list of FBI and State Police

The hospital worked with Inc., to take the site down according to the Sun. Many people saw the

Kinney said there was a system that allowed plans to send a letter

### University of Idaho

UI Home

Vandal Identity Home

Notification Letter

Frequently Asked Questions

Resources

News Release

Phone Bank

## Vandal Identity Res

In February 2007, a file containing data for research purposes was posted to the Internet outside of the University. The file was removed by the Services office immediately upon disclosure. Information for University employees, including Social Security numbers, was included in the file. The file did not include any personal information.

To date, the university has no indication of the reason for which it was breached, and is recommending steps to protect individuals and recommending steps to

We recommend that you take measures to protect your information by utilizing services available at [www.annualcreditreport.com](http://www.annualcreditreport.com) and clicking on the "Vandal Identity Res

The University of Idaho has established a phone bank as part of its response to this incident. The phone bank can relay questions not addressed on this Web site to the university's incident response team.

The phone bank operates Monday through Friday, 8 a.m. to 5 p.m. Pacific. Call toll free at (888) 900-3783 or in Moscow (208) 885-2082.



tj-max

Marshalls

HomeGoods

A.J.Wright

WINNERS

HOMESENSE

TJ-max



## LETTER FROM TJX'S PRESIDENT AND CEO

February 21, 2007

To Our Valued Customers:

As TJX's President and Chief Executive Officer, I want our customers to know how much I personally regret any difficulties you may experience as a result of the unauthorized intrusion into our computer systems. We are working with leading computer security firms to investigate the problem and enhance our computer security in order to protect our customers' data. We are dedicating significant resources to evaluate the issue. Given the nature of the breach, the size and international scope of our operations and the complexity of the way credit card transactions are processed, the evaluation is, by necessity, taking time.

Since we learned of the probability of a breach in mid-December 2006, we have cooperated with law enforcement as well as with the banks and credit card companies that process our customer transactions. Further, we have established customer helplines in three countries and are making available a great deal of helpful information on our company websites.

We are committed to continue to address the situation and to provide periodic updates as we learn more. We have reported updated information in a press release which you will find below.

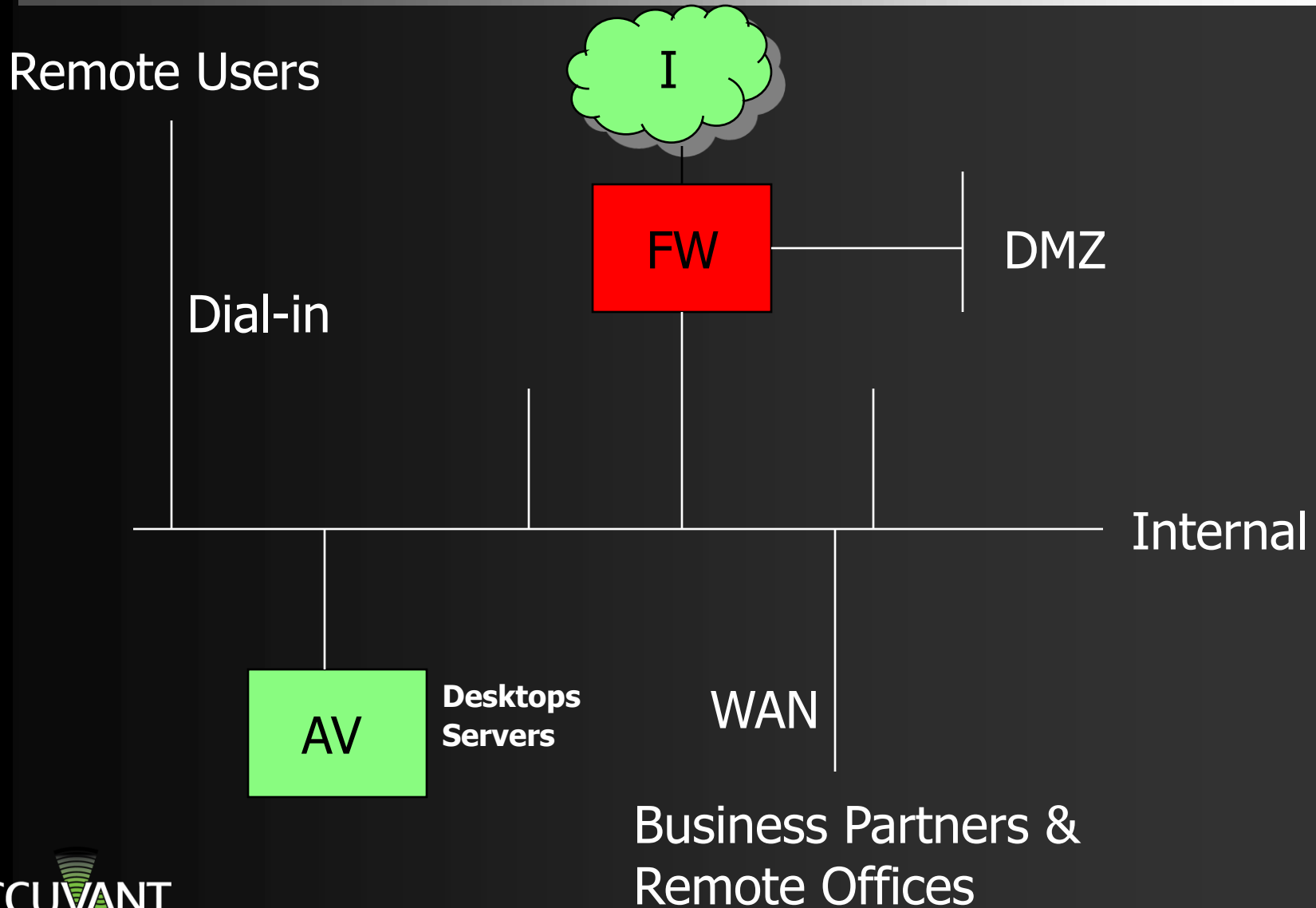
Additionally, I encourage you to access the information we are providing on this website to learn more about steps you can take to protect your credit and debit card information, or to contact our special customer helplines.

With the help of computer security experts, we have strengthened the security of our computer systems and we believe customers should feel safe shopping in our stores. We value the trust our customers place in us and again, I'd like you to know that we sincerely apologize for any difficulties you may be caused. Thank you for continuing to shop at our stores and for your years of loyal patronage.

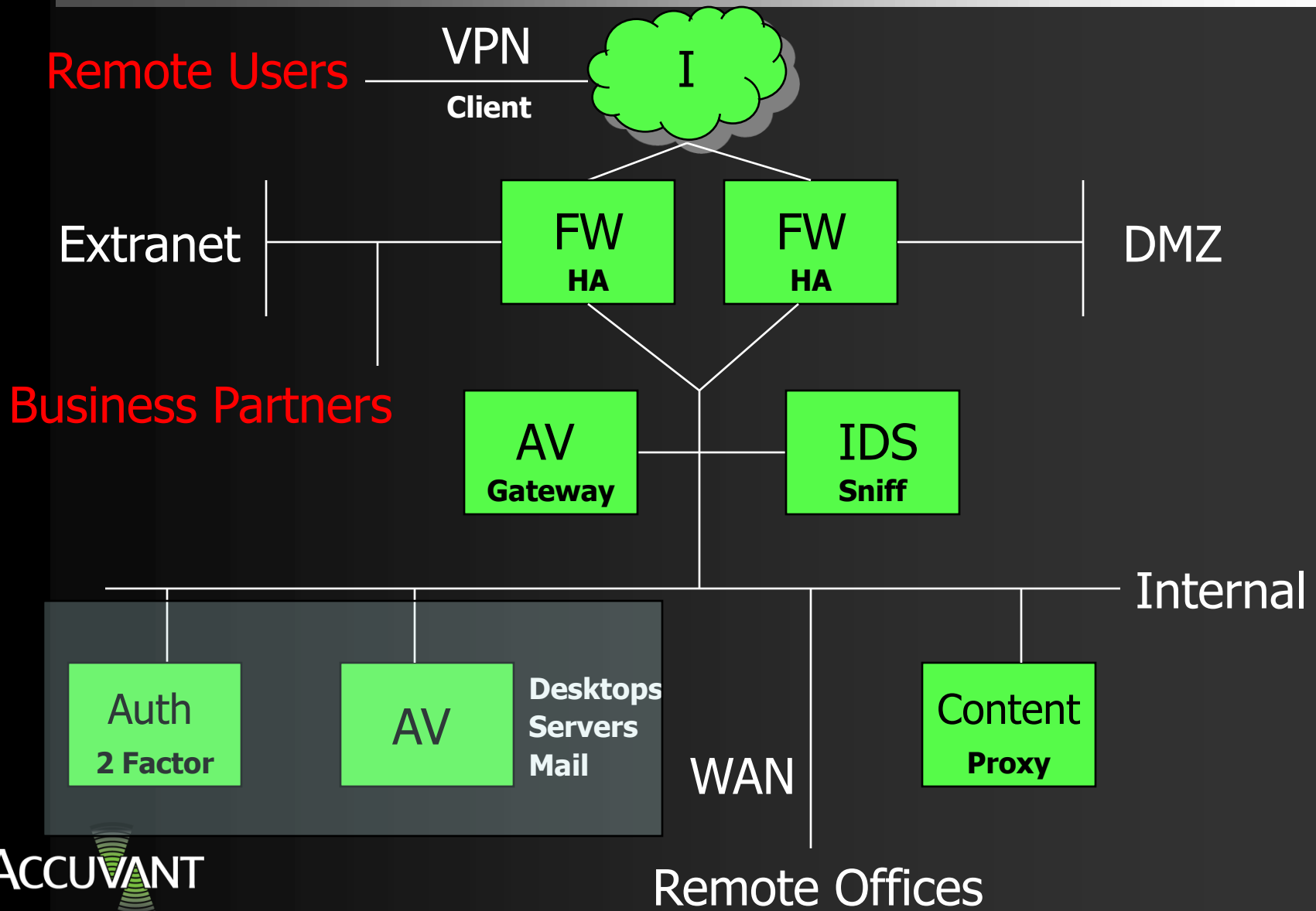
Respectfully,

Carol Meyrowitz  
President and Chief Executive Officer

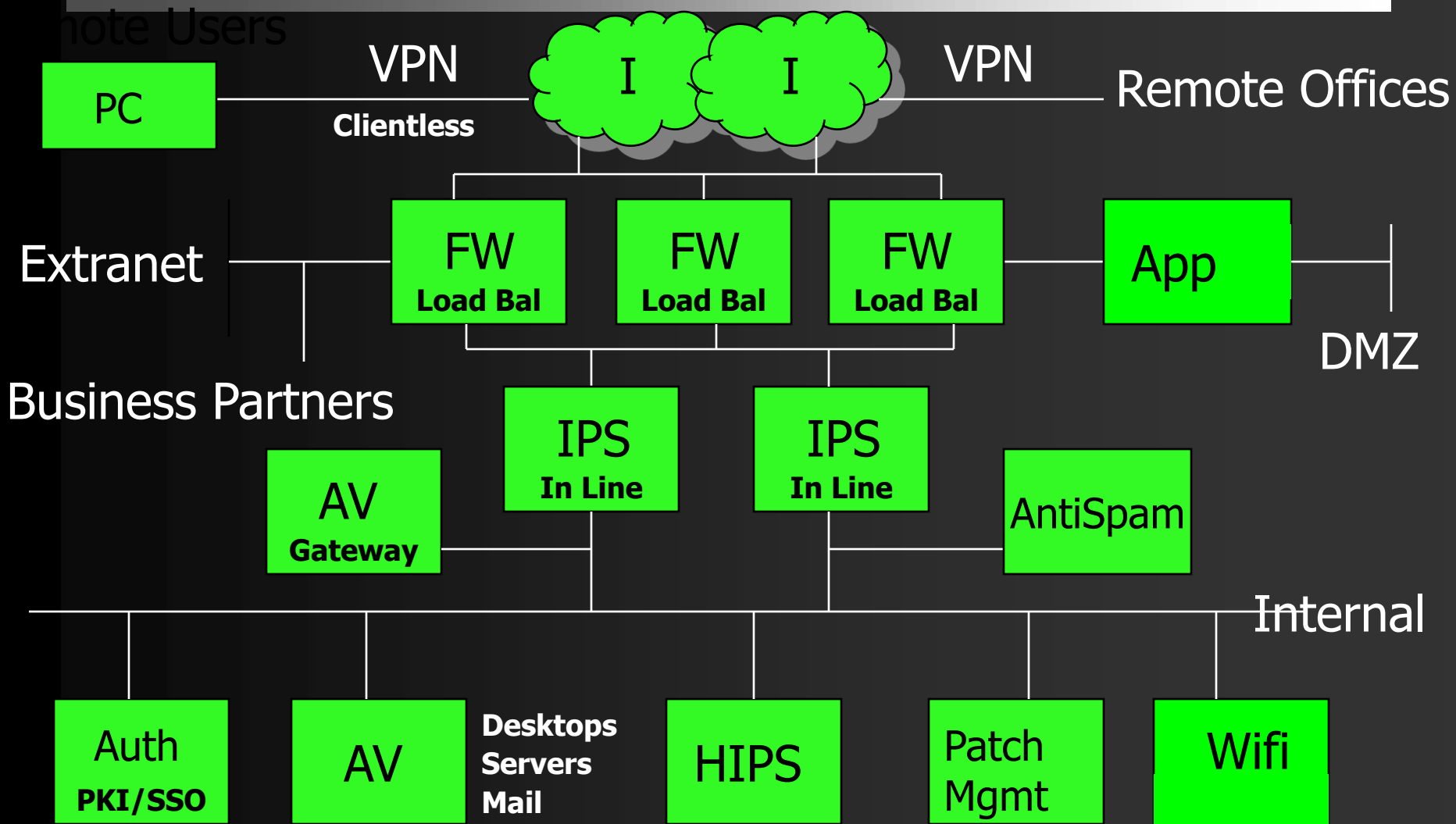
# Security Architecture - 1999



# Security Architecture - 2001



# Security Architecture - 2007

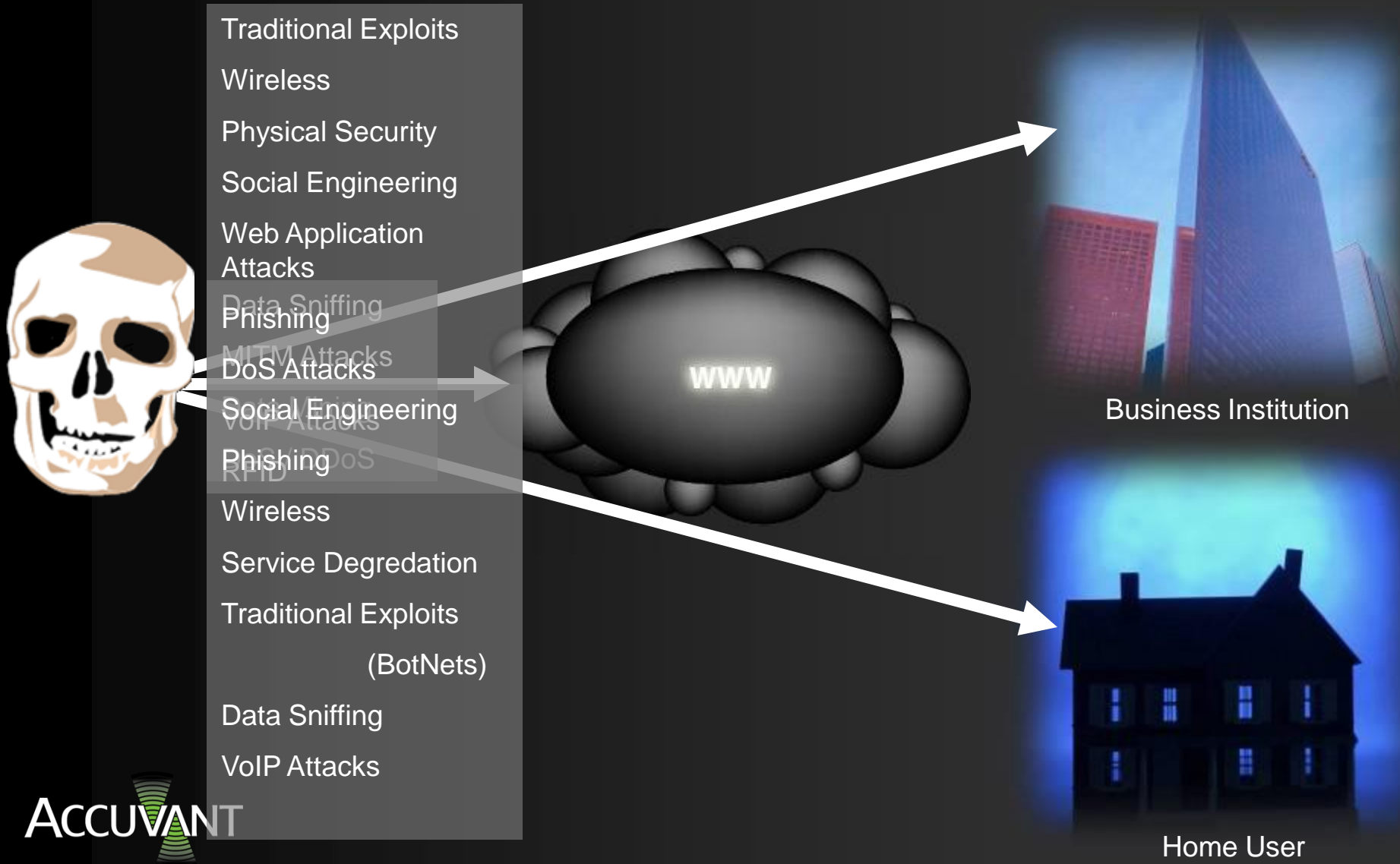


---

As Architectures Have Changed,  
So Have the Hackers Techniques

# Understanding Our Perimeter...

## Where are the Threats?



# Data Mining and Target Identification

---

- Google Hacking
  - Introduced in 2003 by Johnny Long – [johnny.ihackstuff.com](http://johnny.ihackstuff.com)
  - Takes advantage of Google’s spidering capability along with finely crafted search queries to find information on the web
    - intitle: | allinurl: | intext: | filetype:
  - Targeting:
    - Sensitive Information
    - Data Mining “Usernames and Passwords”
    - Finding Vulnerable Targets (Error Messages, Banners, etc.)
    - Driver for web application worms

# Using Google to Identify Targets

---

## Demonstration

# You may not be looking for trouble...

---

## Public Data Leakage Solutions

- Never leave unnecessary files on a web server (i.e. Web.config.old, password.log)
- Assume all files on a web server will be seen by a someone with malicious intent
- Encrypt sensitive information in configuration files

# Traditional Exploits Tools & Techniques

- Public Code / Reverse engineering
  - Patch Tuesday = Exploit Wednesday
- Frequently the target of Virus' and Worms
- Exploit Frameworks
  - MetaSploit
  - Canvas (Immunity Security)
  - Mosquito
  - IMPACT (CORE technologies)

# Traditional Exploits— Exploit Frameworks




EXPLOITS      PAYLOADS      SESSIONS

Filter Modules

- 3Com 3CDAemon FTP Server Overflow
- AOL Instant Messenger goaway Overflow
- \* AWStats configdir Remote Command Execution
- Alt-N WebAdmin USER Buffer Overflow
- Apache Win32 Chunked Encoding
- AppleFileServer LoginExt PathName Overflow
- \* Arkeia Backup Client Remote Access
- Arkeia Backup Client Type 77 Overflow (Mac OS X)
- Arkeia Backup Client Type 77 Overflow (Win32)

```
Unreal Tournament 2004 "secure" Overflow (Win32)
War-FTPD 1.65 PASS Overflow
War-FTPD 1.65 USER Overflow
WebSTAR FTP Server USER Overflow
Microsoft SSL PCT MS04-011 Overflow
Microsoft WINS MS04-045 Code Execution
WS-FTP Server 5.03 MKD Overflow
ZENworks 6.5 Desktop/Server Management Remote S
rgets', 'payloads', 'options', or 'advanced'
rgets
```

- globalscapertp\_user\_input GlobalSCAPE Secure FTP Server user input ove
- gnu\_mailutils\_imap4d GNU Mailutils imap4d Format String Vulnerab
- hpux\_ftpd\_preauth\_list HP-UX FTP Server Preauthentication Directory
- hpux\_lpd\_exec HP-UX LPD Command Execution
- ia\_webmail IA WebMail 3.x Buffer Overflow
- icecast\_header Icecast (<= 2.0.1) Header Overwrite (win32)
- ie\_objecttype Internet Explorer Object Type Overflow
- iis40\_hdr IIS 4.0 .HTB Buffer Overflow
- iis50\_printer\_overflow IIS 5.0 Printer Buffer Overflow
- iis50\_webdav\_ntdll IIS 5.0 WebDAV ntdll.dll Overflow
- iis\_fp30reg\_chunked IIS FrontPage fp30reg.dll Chunked Overflow
- iis\_nsislog\_post IIS nsislog.dll ISAPI POST Overflow
- iis\_source\_dumper IIS Web Application Source Code Disclosure
- iis\_v3who\_overflow IIS v3who.dll ISAPI Overflow
- imail\_imap\_delete IMail IMAP4D Delete Overflow
- imail\_lmtp IMail LMTP Service Buffer Overflow
- irix\_lpsched\_exec IRIX lpsched Command Execution
- lsass\_ms04\_011 Microsoft LSASS MS04-011 Overflow
- mailenable\_auth\_header MailEnable Authorization Header Buffer Overf
- mailenable\_imap MailEnable Pro (1.54) IMAP SELECT Request Buffer
- maxdb\_webdbm\_get\_overflow MaxDB WebDBM GET Buffer Overflow



EXPLOITS      PAYLOADS      SESSIONS

Microsoft SSL PCT MS04-011 Overflow (win32\_bind)

PROTO	Optional	DATA	raw	The application protocol (raw or snrtp)
RHOST	Required	ADDR		The target address
RPORT	Required	PORT	443	The target port
EXITFUNC	Required	DATA	thread	Exit technique: 'process', 'thread', 'seh'
LPORT	Required	PORT	4444	Listening port for bind shell

Preferred Encoder: Default Encoder

Ngsp Generator: Default Generator

-Check-   -Exploit-

COPYRIGHT © 2003-2005 METASPLOIT.COM

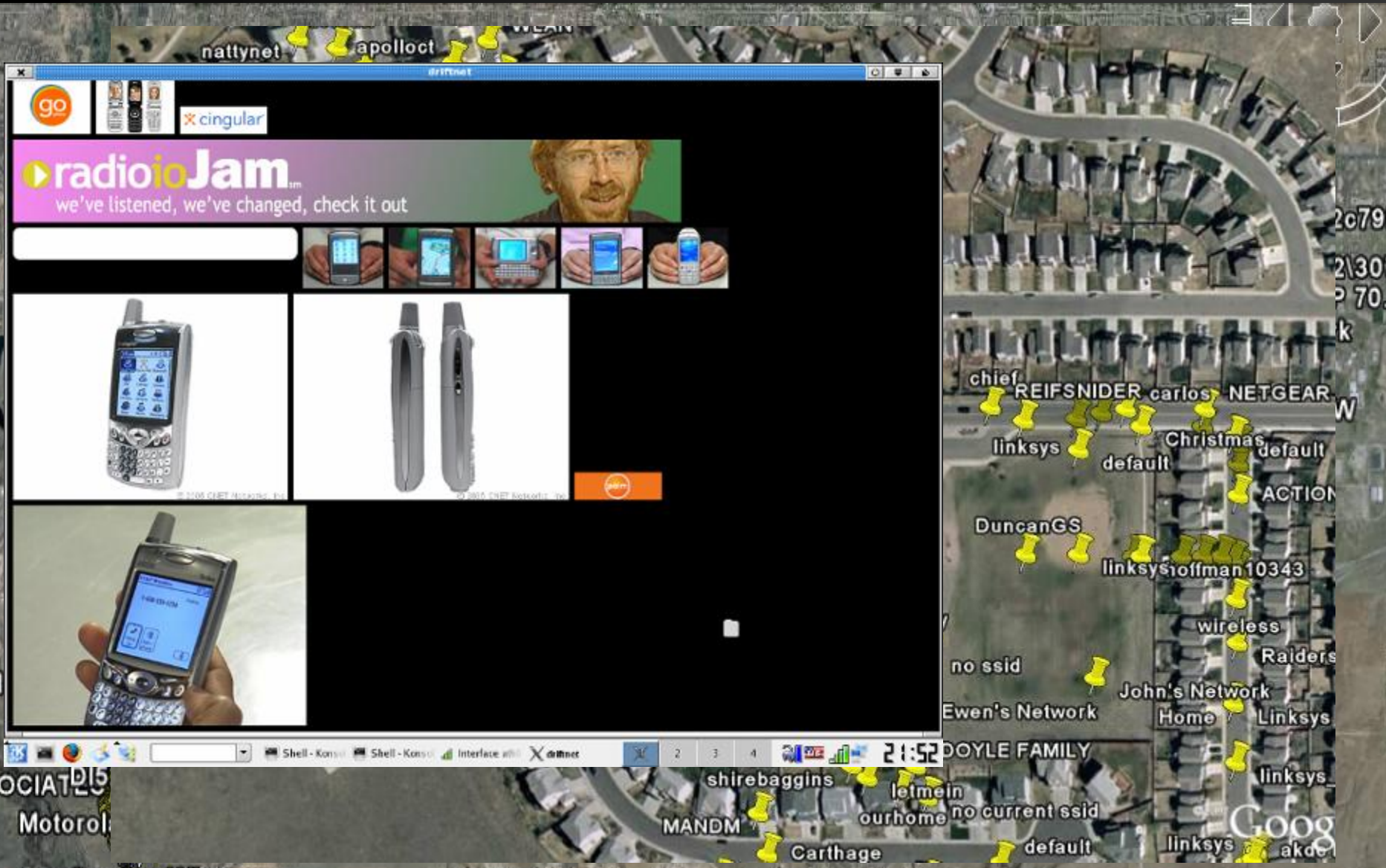
msf windows\_ssl\_pct >

# Traditional Exploit Solutions

---

- MUST have streamlined patching procedures
- MUST have an inventory process
  - Include Asset Criticality
  - Include Exposure Levels (inbound & outbound)
- MUST have vulnerability management standards and procedures in place

# Attacking Wireless Networks



SOCIATIS  
Motorol

Gundan Wing

# Cracking Wireless Using Freely Available Tools

---

Demonstration

# Wireless Solutions

---

- Strong Authentication
- Strong Encryption
- Protect client systems
- Wireless IPS
- Modern Technologies

# Web Application Targeting

---

## Manipulating the Way Things are 'Supposed' to Work

- Web Application Attacks
  - On average, 90% of all dynamic content sites have vulnerabilities associated with them.
    - “Today over **70%** of attacks against a company’s network come at the ‘Application Layer’ not the Network or System layer.” - *Gartner*
  - These attacks occur due to the applications inability to prevent a user from modifying data submitted to the site – post-browser / pre-server
    - SQL Injection
    - Parameter Manipulation
    - Session Mgt / Privilege Escalation
    - Error Handling
    - Denial of Service

# Application Vulnerabilities

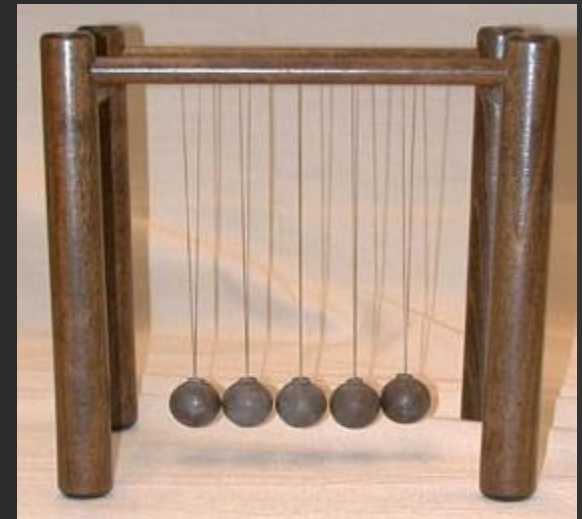
---

Demonstration

# Physical Security Attacks – Key Bumping

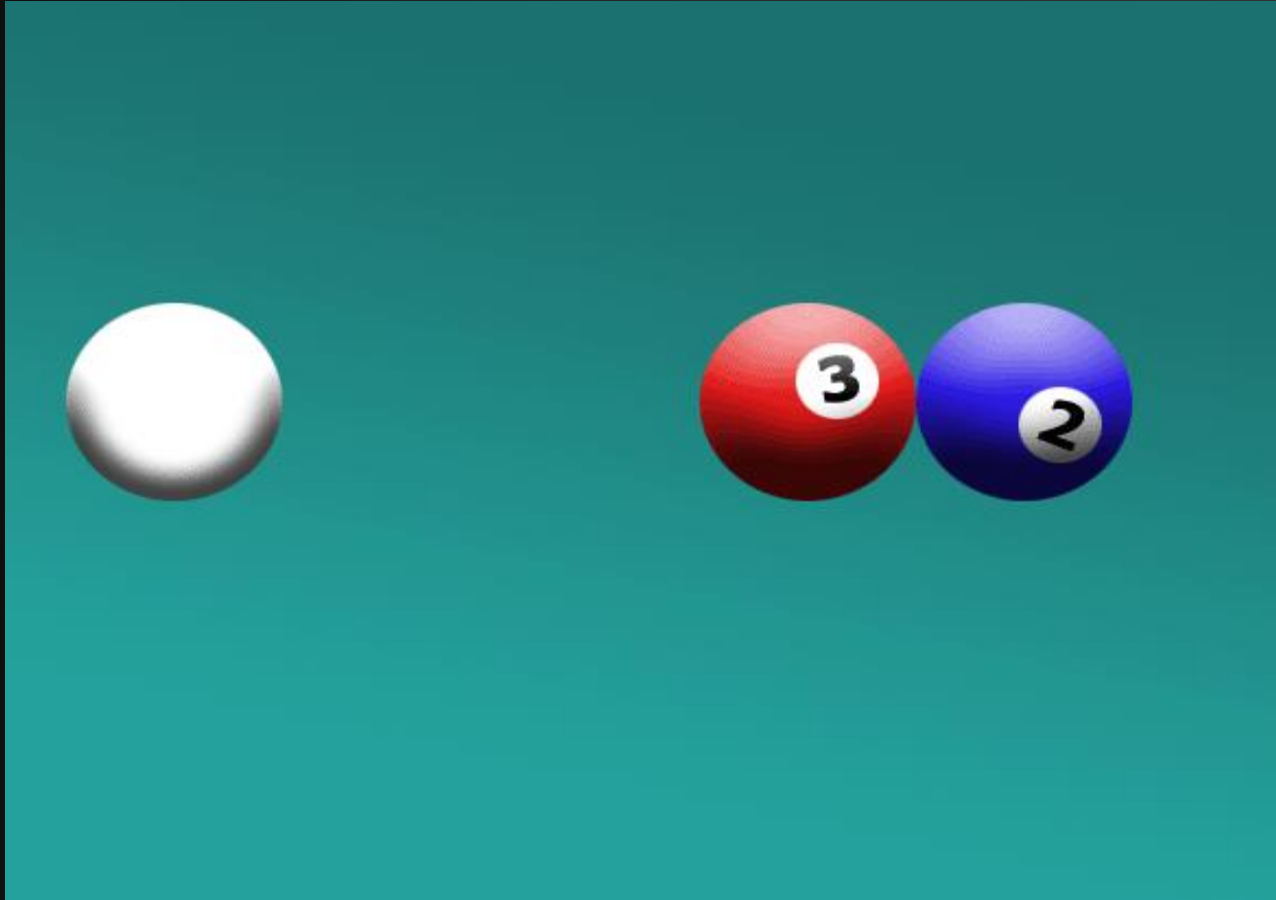
## Once Physical Access is Obtained...It's Game Over

- Bumping Technique –
  - Specialized keys
  - Newton's cradle principle
  - Related to pick gun lock picking method

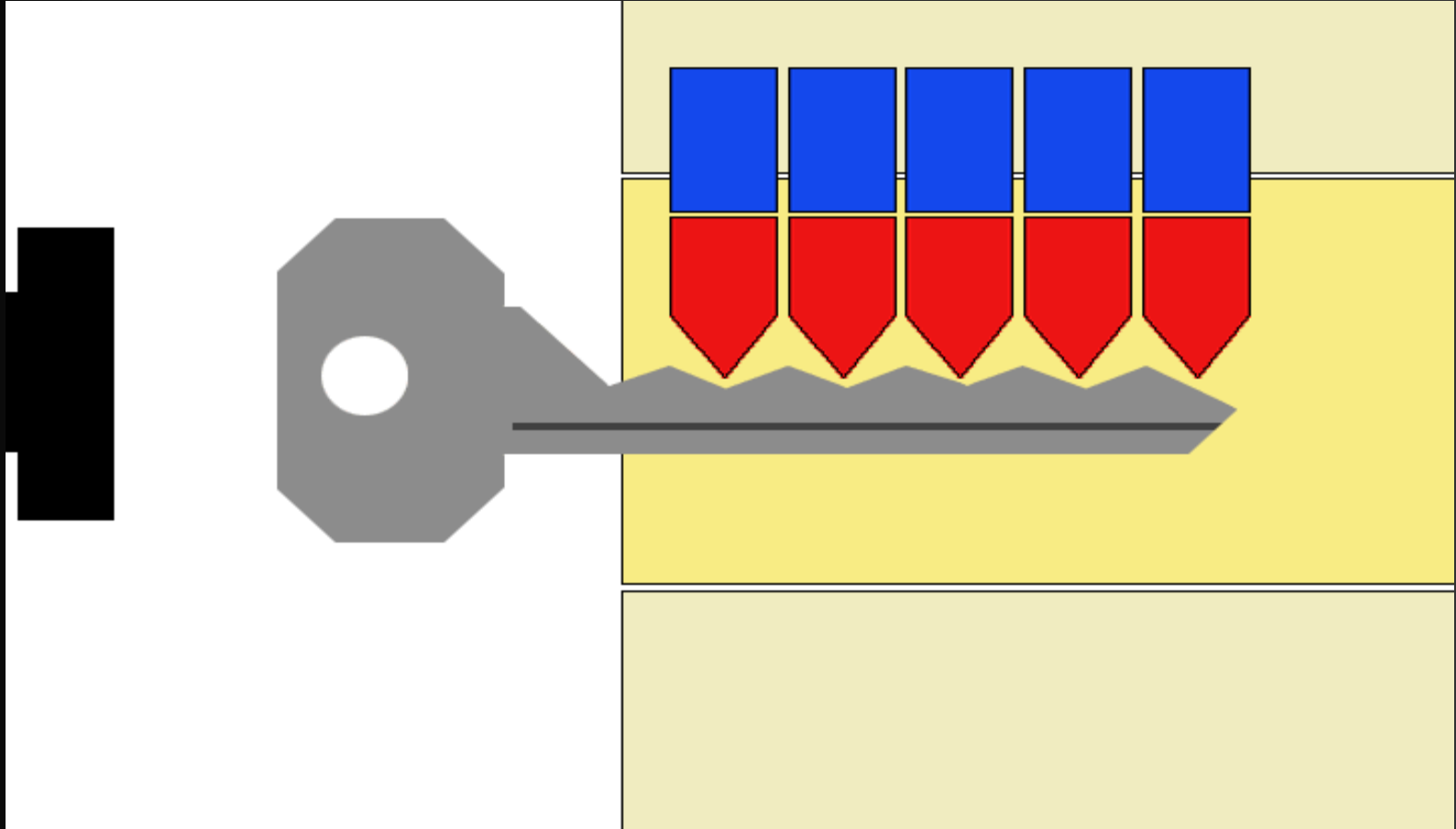


# How Bumping Works

---



# Key Bumping

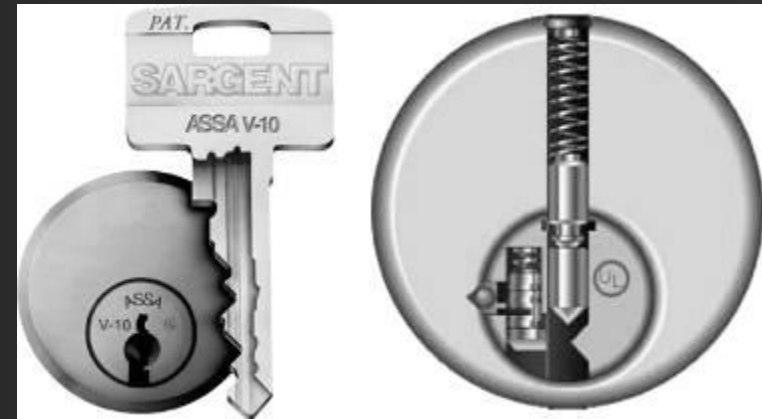


---

# Demonstration

# Key Bumping Threat

- High Level of Risk
  - Inexpensive
  - Inconspicuous
  - EASY
  - Few locks offer protection
    - Especially in the USA
      - Sidebars
      - Trap Pins
      - Shadow Drilling
  - Insurance problems



# VoIP

---

- VoIP Implementations Becoming Prolific
- Security / Stability / Availability are Critical for Consumer Experience / Brand Reputation
- Attack Vectors:
  - Traditional Exploits
  - QoS/DoS Attacks
  - Call HiJacking
    - Evesdropping
    - Manipulation
  - VoIP Phishing
    - Identity Theft

---

# Demonstration

# VoIP / Fun Phone Games

- With the installation of VoIP solutions, older phone issues are now having to be re-addressed
- Attack Vectors:
  - Caller ID Spoofing
    - VM theft
    - Social Engineering
  - 911 systems



The screenshot shows the SpoofCard website control panel. The header features the SpoofCard logo with the tagline "BE WHO YOU WANT TO BE". Below the header, there is a "Listen To Recording" section with a "Delete Recording" button. Below this, there is a "Download File To Computer" section with a note: "(Right click on above link and Select 'Save Target As')". Below the download section, there is a table with the following data:

Called	Call Date	Length	Cost	File Size
13033593954	3/13/2007 7:03:38 PM	1:30 min	\$0.33	78.49 kb

On the right side of the control panel, there is a "Calling Card Balance: \$6.17" section. Below this, there is a list of menu items: "VIEW CALL LOG", "SET PREFERENCES", "ADD MONEY TO ACCOUNT", "VIEW PAYMENT HISTORY", "CUSTOMER SERVICE", and "LOG OUT". At the bottom right, there is a circular button that says "JOIN OUR AFFILIATE PROGRAM & EARN" with an image of hands holding money.

Copyright (c) 2006, Spoof Card. All rights reserved.

---

# Demonstration

# VoIP Defense Strategies

---

- Follow the Basics:
  - Robust Architecture
  - Defense-in-Depth
- Avoiding Being a Victim
  - Set Passwords on your accounts
  - Never believe Caller-ID
  - Never give out any sensitive information to someone who calls you or as a return call to an un-validated source
  - Validate any information with pertinent institution

# RFID

- RFID has been in use for a while but now is being put into “everything”
- Uses include retail, manufacturing, animal identification, to access control
- Attack Vectors:
  - Asset Tracking / Data Modification
  - SQL Injection (just like web apps)
  - Cloning



---

# Demonstration

# RFID Defense Strategies

---

- Follow the Basics:
  - As with all RF know your footprint and placements.
  - Follow the technology - upgrade when needed
- Avoiding Being a Victim
  - If you can't upgrade to a newer technology (such as I-Class) change out the entry panels with ones that use TAG+Passcode.

# Conclusions

---

- Understanding where the attacks are coming from and where you are vulnerable is the first step to protecting your assets, your customers and your reputation
- Perimeter security requires a clear understanding of the perimeter and where you are exposed
  - Secure Applications
  - Secure Wireless
  - Secure Facilities
  - Defense-in-Depth
- There is no security through obscurity
- Vulnerabilities are coming out faster and exploitation is getting easier

---

# Questions?